ARO 24649.6-EL-S

NETWORK ANALYZER FOR NONSTATIC JAMMING

Interim Technical Report

Axiomatix

NETWORK ANALYZER FOR NONSTATIC JAMMING

Interim Technical Report

Unjeng Cheng

June 30, 1989

U. S. Army Research Office
P. O. Box 12211
Research Triangle Park, NC 27709-2211

Contract No. DAAL 03-87-C-0007

Axiomatix
9841 Airport Boulevard
Suite 1130
Los Angeles, CA 90045

Axiomatix Report No. R8906-3

TABLE OF CONTENTS

AD-A210 759

DTIC FILE COPY

2

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER ARO 24649.6-EL-S	2. GOVT ACCESSION NO. NA	3. RECIPIENT'S CATALOG NUMBER NA
4. TITLE (and Subtitle) NETWORK ANALYZER FOR NONSTATIC JAMMING		5. TYPE OF REPORT & PERIOD COVERED Interim
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Unjeng Cheng		8. CONTRACT OR GRANT NUMBER(s) DAAL03-87-C-0007
9. PERFORMING ORGANIZATION NAME AND ADDRESS Axiomatix 9841 Airport Blvd., Suite 1130 Los Angeles, CA 90045		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS NA
11. CONTROLLING OFFICE NAME AND ADDRESS U. S. Army Research Office P. O. Box 12211 Research Triangle Park, NC 27709-2211		12. REPORT DATE June 30, 1989
		13. NUMBER OF PAGES 19
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

DTIC ELECTE AUG 0 2 1989 S D

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

NA

18. SUPPLEMENTARY NOTES

The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Adaptive Networks, Code-Division-Multiple-Access (CDMA), Communications, Networks, Network Simulation, Nonstatic Jamming, Packet Radio, Spread Spectrum

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report describes a network analyzer for the PRNET's under nonstatic jamming attack. The analyzer is based on the QNA algorithm and a modified traffic concept. The effect on network operation due to the blocked packet handling scheme is investigated. The effects of dead-ends and looping on the busy probability are also investigated.

I. INTRODUCTION

The survivability of a packet radio network (PRNET) under jamming attack is an important issue. The goal of this research is to develop the analytical methods for understanding as well as predicting the behavior of PRNETs under various jamming conditions. Jamming can be stationary or nonstationary. For the stationary jamming, the jamming strategy is fixed, but it can be described stochastically. For instance, we may say that a node is jammed with probability 0.5 in each slot. Therefore, although the jamming strategy is fixed, the actual jamming pattern changes from slot to slot. A subclass of the stationary jamming is the static jamming, where the jamming pattern is fixed. For the nonstationary jamming, the jamming strategy changes from time to time. A subclass of the nonstationary jamming is the nonstatic jamming, where a fixed jamming pattern is applied in each block of time, but the jamming pattern changes from block to block. We analyzed the behavior of PRNETs under static jamming attack in our previous report [1]. In this report, we introduce a method for analyzing the PRNET behavior under the nonstatic jamming attack.

The analytical results for the static jamming attack scenario were presented in [1] for both the transmitter-based code and the receiver-based code networks. The numerical results were given only for the receiver-based code case. Simulations were performed to verify the accuracy of the analytical approach. The analytical methods are based on the queueing network analyzer (QNA) algorithm [2] and the Silvester-and-Lee (SL) algorithm [3]. The accuracies of the QNA and SL algorithms were compared in [1]. We show that both algorithms provide accurate results in the light traffic conditions and the QNA algorithm is more accurate than the SL algorithm in the heavy traffic conditions.

A simple form of nonstatic jamming is the periodic block jamming, where finite number of jamming patterns are used by the jammers following a fixed sequence and are repeated indefinitely. If the period is long and the set of jamming patterns is large, a periodic jamming attack resembles a finite-length random block jamming. The periodicity

makes the underlined processes recurrent; thus, a simulation study is possible. The window-averaging concept described in [1,4] provides a way to delineate the network behavior under the periodic block jamming attack. The simulation results presented in [4] demonstrated the technique, where the window size is the same as the length of the network information exchange interval. We considered both the node busy probability and the node packet delay. The average node packet delay at a node in a window is obtained by considering all packets arriving at the node in that window. We showed that the node busy probability and the node packet delay can change significantly from window to window. The simulation results showed the existence of the worst case jamming, which depends on the traffic pattern, the jamming strategies, the link quality monitoring, and the adaptive routing algorithm.

For the periodic block jamming with a long period, excessive simulation time is needed to obtain the reliable results. Therefore, we need an analytical tool to quickly give us the insight of the network behavior under the nonstatic jamming attack. A good analytical tool should be able to predict the network performance from window to window, to find the worst case jamming, and to evaluate the performance of the adaptive routing algorithms.

The formulation presented in this report is based on the QNA algorithm. We assume that the observation window size is the same as the length of the network information exchange interval and the observation windows are synchronous with the information exchange intervals. We first note that an adaptive network under the block jamming attack does not have a permanent equilibrium state. However, if the window size is large, i.e., each window contains many slots, a short-term equilibrium state could be reached by the network in a window. When this is true, we can apply the QNA algorithm to find the equilibrium solutions in that window. For an adaptive network under the nonstatic jamming attack, some source-destination pairs may not have routes between them at certain moment. When this happens, the network has no equilibrium state in that

window and the QNA algorithm does not converge. In the subsequent discussion, we present a method to find an approximate solution for this case.

The traffic between a blocked source-destination pair is referred to as the blocked traffic. The traffic between an unblocked source-destination pair is referred to as the unblocked traffic. Whether a source-destination pair is blocked or unblocked in an observation window is determined by the routing table and the jamming topology in that window. If a network contains only the unblocked traffic, its equilibrium solution can exist. A network with the blocked traffic does not have a equilibrium solution simply because of its blocked traffic. To find the solution in the block conditions, we must consider the blocked and the unblocked traffic differently. Before we proceed further, we observe that the nodes processing only the unblocked traffic can reach their respective equilibrium state, but the nodes processing some blocked traffic many not have equilibrium state at all. The QNA algorithm does not converge simply because of those nodes having no equilibrium state. This observation is the basis of our theory presented in the following.

In section II, we illustrate a model for the blocked traffic. In section III, we examine the key features of an adaptive routing algorithm and their roles in the analyzer. In this section, we also address five methods to handle the blocked traffic and discuss their influence on the network operation. In section IV, we consider the effect of a dead-end on the busy probability. In section V, we consider the effect of looping on the busy probability. The conclusions and future research are given in secion VI.

II. A MODEL FOR THE BLOCKED TRAFFIC

The blocked traffic enter and flow through the network in the same way as the unblocked traffic until they hit a dead-end or until they begin to loop around. Both a dead-end and looping are referred to as an ill-conditioned end. Intuitively, the solution for a network with the blocked traffic consists of three components: (1) the equilibrium solution due to the blocked traffic before hitting an ill-conditioned end and the unblocked traffic, (2) the transient solution due to the blocked traffic at an ill-conditioned end, and (3) the interaction between the unblocked traffic and the blocked traffic at an ill-conditioned end. We also note that the scheme to handle the blocked traffic does affect the solution, which is the subject of section III. In this section, we consider only the equilibrium solution component.

To obtain the equilibrium solution component, we first modify the traffic pattern by changing the destination nodes of all blocked traffic. For each blocked source-destination pair, the new destination node will be the last node along the respective route before an ill-conditioned end. Thus, the blocked traffic can flow through the network as usual and is absorbed at an ill-conditioned end. The sum of the unblocked traffic and the modified blocked traffic is referred to as the modified traffic. We find the equilibrium solution of the network with the modified traffic using the QNA algorithm.

We use two examples to illustrate the concept of the modified traffic. The first example illustrates the effect of a dead-end and the second example illustrates the effect of looping. Let us first consider the network shown in Figure 1. The traffic matrix is given in Figure 1(b). Suppose that in a particular observation window, the network has the routing table shown in 1(c), and the jammer begins to jam node 3 at the beginning of this window. Then the traffic $\gamma_{1,3}$, $\gamma_{1,4}$, $\gamma_{2,3}$, $\gamma_{2,4}$, $\gamma_{4,1}$, $\gamma_{4,2}$, $\gamma_{4,3}$, and $\gamma_{5,3}$ are blocked by jamming. The traffic $\gamma_{1,3}$ and $\gamma_{1,4}$ flow from node 1 to node 2 as usual, but they are blocked at node 2. Thus, the modified traffic $\gamma'_{1,2}$, from node 1 to node 2 is given by $\gamma'_{1,2} = \gamma_{1,2} + \gamma_{1,3} + \gamma_{1,4}$. The traffic $\gamma_{2,3}$ and $\gamma_{2,4}$ are blocked at their entrance, i.e.,

node 2. Since they do not flow through the network at all, they should not be included in the modified traffic. After examining the traffic between every source-destination pair, the resulting modified traffic matrix is shown in Figure 1(d).

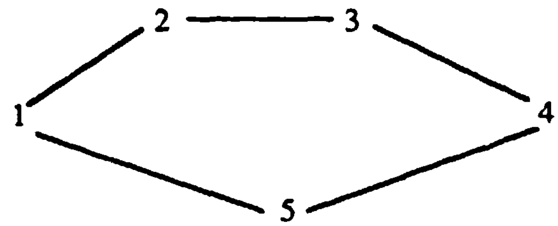

Figure 1(a). The First Example.

$\gamma_{i,j}$	1	2	3	4	5
1	0	0.02	0.02	0.02	0.02
2	0.02	0	0.02	0.02	0.02
3	0.02	0.02	0	0.02	0.02
4	0.02	0.02	0.02	0	0.02
5	0.02	0.02	0.02	0.02	0

Figure 1(b). The Traffic Matrix.

Source-Destination	Route	Source-Destination	Route
1 - 2	1 → 2	3 - 4	3 → 4
1 - 3	1 → 2 → 3	3 - 5	3 → 4 → 5
1 - 4	1 → 2 → 3 → 4	4 - 1	4 → 3 → 2 → 1
1 - 5	1 → 5	4 - 2	4 → 3 → 2
2 - 1	2 → 1	4 - 3	4 → 3
2 - 3	2 → 3	4 - 5	4 → 5
2 - 4	2 → 3 → 4	5 - 1	5 → 1
2 - 5	2 → 1 → 5	5 - 2	5 → 1 → 2
3 - 1	3 → 2 → 1	5 - 3	5 → 4 → 3
3 - 2	3 → 2	5 - 4	5 → 4

Figure 1(c). The Routing Table.

$\gamma'_{i,j}$	1	2	3	4	5
1	0 (0.0)	$\gamma_{1,2}+\gamma_{1,3}+\gamma_{1,4}$ (0.06)	0 (0.0)	0 (0.0)	$\gamma_{1,5}$ (0.02)
2	$\gamma_{2,1}$ (0.02)	0 (0.0)	0 (0.0)	0 (0.0)	$\gamma_{2,5}$ (0.02)
3	$\gamma_{3,1}$ (0.02)	$\gamma_{3,2}$ (0.02)	0 (0.0)	$\gamma_{3,4}$ (0.02)	$\gamma_{3,5}$ (0.02)
4	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	$\gamma_{4,5}$ (0.02)
5	$\gamma_{5,1}$ (0.02)	$\gamma_{5,2}$ (0.02)	0 (0.0)	$\gamma_{5,3}+\gamma_{5,4}$ (0.04)	0 (0.0)

Figure 1(d). The Modified Traffic Matrix.

Next, let us consider the example shown in Figure 2. Suppose that in a particular observation window, the traffic $\gamma_{1,4}$ is flowing along the $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$ route, and the jammer begins to jam node 3 at the beginning of this window and continues to jam node 3 in the following windows. In the first observation window, the traffic $\gamma_{1,4}$ hits a dead-end at node 2; thus, the modified traffic $\gamma'_{1,2}$ should include $\gamma_{1,4}$. However, the route for $\gamma_{i,4}$ may change from window to window because of the adaptive routing algorithm. Suppose that after several routing information exchanges, a loop is created along the route for $\gamma_{1,4}$, namely, the route is $1 \rightarrow 2 \rightarrow 11 \rightarrow 12 \rightarrow 13 \rightarrow 14 \rightarrow 2$. For this case, the traffic $\gamma_{1,4}$ flows through nodes 1, 2, 11, 12, 13, and 14 as usual. After node 14, the traffic $\gamma_{1,4}$ flows back to node 2 and begin to loop. Thus, the modified traffic $\gamma'_{1,14}$ should include the traffic $\gamma_{1,4}$.

Using the modified traffic concept, the equilibrium solution component provides an approximate solution for the nodes which have equilibrium state. The next issue is to find an approximate solution for the nodes which do not have the equilibrium state; these nodes are referred to as the transient nodes. The transient nodes include the nodes which are a dead-end of some blocked route and the nodes in the loop of some blocked route. Clearly,

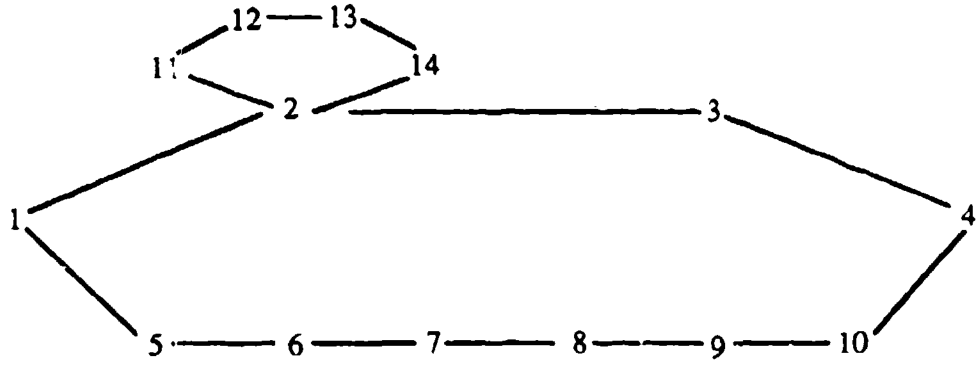

Figure 2. Second Example.

the transient nodes have no equilibrium because of the continuous accumulation of the blocked packets in them. Therefore, the scheme to handle the blocked packets will influence the transient solution. This is our subject in the next section.

III. ASPECTS OF ADAPTIVE ROUTING ALGORITHMS

The basic functions of the routing algorithms for PRNETs include (1) channel quality monitoring, (2) routing information exchange, and (3) routing table computation. Many other supporting functions are also needed for an operational routing algorithm. For instance, a node may have to identify itself periodically if it is idle over significant number of slots. An ideal analytical tool should take into account as many functions as possible. However, the complexity of the adaptive routing algorithms makes this attempt impossible. In order to be analytically tractable, we must begin with the model including only the basic functions.

Let us first examine the channel monitoring scheme. Generally speaking, the quality of a link is a function of the jammer power. The accuracy of the link quality measurement is determined by the number of packets passing the link. The bad-link-detection-threshold will definitely influence the decision of the adaptive routing algorithm in every routing table computation. Therefore, the actual route chosen for each source-destination pair in each observation window depends on the current jammer power, the current jamming topology, the traffic distribution, and the bad-link-detection-threshold. Such a complex process can only be determined by simulation. Furthermore, the complexity of simulation also varies significantly, depending on the assumption we make. The following two scenarios simplify the simulation task in different magnitudes.

<u>Channel Monitoring Scenario #1:</u>

We assume that the jammer power is very strong when it is on. Thus, the jammed node cannot receive any data packet successfully. The jammed links will be detected within one observation window and will be declared bad with probability 1. We also assume that the links not jammed are always declared good following the measurement in each observation window.

Channel Monitoring Scenario #2:

There is no constraint on the jammer power. However, the amount of traffic flowing through each node is always adequate so that each node can obtain the link quality measurement precisely.

In scenario #1, the jammed links are always detected and declared bad and the links not jammed are always declared good. Therefore, whenever the jamming topology changes, the routing table changes accordingly in the next observation window. This makes the simulation of the interaction between the routing algorithm and the jamming straightforward.

In scenario #2, the jammed links may not be declared bad and the links not jammed may not be declared good. The adaptive routing algorithm responds to the jamming topology change in an stochastic manner. Since the probability for a link being declared bad can be expressed analytically in terms of the jamming power and the signal-to-thermal-noise ratio, there is no difficulty to simulate the interaction between the routing algorithm and the jamming strategy. Because of the stochastic behavior of the adaptive routing algorithm, the problem under scenario #2 is more complex than the problem under scenario #1.

Finally, if the amount of traffic flowing through each node is not enough for accurate link quality measurement, then the probability for a link being declared bad cannot be expressed in a closed form. Thus, the link quality measurement must be obtained by simulating the traffic. Clearly, the problem is significantly more complex than the problem under either scenario #1 or scenario #2. In this report, we will only address scenario #1.

Secondly, let us consider the blocked packet handling schemes. As we mentioned before, the transient nodes are caused by the accumulation of the blocked traffic. Therefore, the way the blocked packets are handled will affect the network behavior significantly. Many schemes are available. Some schemes require each packet carrying its

routing history information. This approach may decrease the link utilization efficiency. Some schemes require each node being equipped with a side buffer. This approach may increase the hardware complexity of each node. In the following, we described five possible approaches:

Non-Removal Scheme:

The blocked packets are handled in the same way as the unblocked packets.

Total-Removal Scheme:

The blocked packets are discarded as soon as they are discovered

Total-Side-Buffer Scheme:

The blocked packets are saved in the side buffer temporarily whenever they are discovered. The packets in the side buffer will be moved back to the transmission buffer as soon as the block condition is resolved.

Dead-End-Removal Scheme:

Only the blocked packets which hit a dead-end are discarded. The other blocked packets are handled in the same way as the unblocked packets.

Partial-Removal Scheme:

The blocked packets which hit a dead-end or enter loops with size equal to or less than a prescribed limit are discarded, where the size of a loop is the number of nodes in the loop. The other blocked packets are handled in the same way as the unblocked packets.

For the Non-Removal scheme, both the blocked and the unblocked packets are in the transmission queue. For the first-come-first-serve scenario, if a dead-end-blocked packet is at the top of the transmission buffer of a node, the outgoing traffic of that node is blocked completely. We also observe that, along a routing loop, the percentage of the

loop-blocked traffic in the total traffic increases with time continuously. Note that all blocked packets stay in the network. As soon as the block condition is resolved, the blocked packets can still reach their destination. The end-to-end packet delay is still the time interval after a packet entering the network and before it leaves the network. The nodes at a dead-end or along the routing loops have no equilibrium solution and we have to derive their transition solution.

The Total-Removal scheme removes all blocked traffic. One way to discover the blocked traffic is to let every packet carry a record of nodes passed by it. Thus, when a node discovers that the next node, to which a particular packet should go, has been visited by that packet before, the packet is removed from the transmission buffer. For this operation scenario, only the modified traffic, including the unblocked traffic and the modified blocked traffic, flow through the networks. Therefore, the equilibrium solution for the network with the modified traffic is valid. However, we must note that the blocked packets are lost in the network. Thus, we need an end-to-end acknowledgement procedure to ensure the successful packet reception at the destination node. The average end-to-end packet delay may contain the end-to-end retransmission delay due to packet loss and it cannot be computed by the QNA algorithm. The equilibrium solution only provides us with the information regarding each node, such as the node busy probability and the average node packet delay.

For the Dead-End-Removal and Partial-Removal schemes, only the nodes along the routing loops of size larger than the prescribed limit do not have the equilibrium solution. In this case, we also need an end-to-end acknowledgement procedure to recover those packets lost in the network.

For the Side-Buffer scheme, the network has an equilibrium state. But the QNA algorithm is not applicable because the packets that form the side buffers are not included in the QNA model. Note that the number of packets in the side buffers depends on the blocked traffic rate and the duration of the block condition. The equilibrium solution for

this case is the same as that for the Total-Removal scheme if we can ignore the traffic fluctuation due to the side buffers; otherwise, other mathematical formulation must be derived. We will not consider this scheme in this report.

Finally, we note that many hybrid schemes can be derived from the aforementioned schemes. The solution for the hybrid schemes can be complex.

The last topic we have to address in this section is how to integrate the routing algorithm with the QNA algorithm. We assume that the routing information exchange and the routing table computation are performed at the beginning of each observation window and the resulting routing tables are used in the entire window. We also assume that if a node is jammed in a window, it is jammed in the entire window. In this study, we consider only the channel monitoring scenario #1. The analyzer for a network under the nonstatic jamming attack follows the following steps:

Step 1: Define the jamming strategy and the traffic matrix.

Step 2: Initialize the routing tables.

Step 3: The routes for each source-destination pair in the current window are computed.

Step 4: The jamming pattern for the current window is derived from the jamming strategy.

Step 5: The modified traffic matrix for the current window is constructed from the traffic matrix and the jamming pattern.

Step 6: The equilibrium solution for the modified traffic is derived by using the QNA algorithm.

Step 7: A transient solution is derived for each transient node.

Step 8: Move to the next observation window. The routing information is exchanged. Every jammed node tells their neighbors that they received nothing in the past window. The routing information include the current routing table used by each node.

Step 9: Every node computes its new routing table according to the received information. then go to Step 3.

We see that this analyzer computes the network performance without using the actual packet flow. Since the strong jammer assumption, the action of the routing algorithm

against the jammer is also deterministic. We can use this analyzer to investigate the characteristics of the underlined adaptive routing algorithm, such as its response speed, its recovery speed, and the associated traffic fluctuation pattern due to the non-static jamming. The output of the analyzer is the average node busy probability and the average node packet delay. At step 7 of the analyzer, we have to find the solution for the transient nodes. Note that step 7 is necessary only if there are transient nodes. For the Total-Removal scheme, there are no transient nodes; thus, step 7 can be omitted.

IV. EFFECT OF DEAD-END ON BUSY PROBABILITY

The blocked packet handling scheme determines what type of blocked conditions may occur in the network. For Non-Removal scheme, both dead-end and looping can occur. For Total-Removal scheme, no blocked conditions may occur. For Partial-Removal scheme, only looping of large size may occur.

Both dead-end and looping destroy the network equilibrium condition. Thus, they cannot be solved by the QNA algorithm. We must consider the problems of dead-end and looping separately. In this section, let us first address the issue of dead-end. The issue of looping is addressed in the next section. Before we proceed, we must mention that the behavior of the transient nodes are complex. In this report, we try to use simple models to explain the transient phenomena. Hopefully, this understanding can lead to more accurate transient analysis in the future.

We consider only the node busy probability in this report. Let us consider the example shown in Figure 1 again. We assume the same scenario described in section II. The blocked traffic $\gamma_{1,3}$ and $\gamma_{1,4}$ hit a dead-end at node 2. We assume the first-come-first-serve discipline at every node; this assumption is the base of the QNA algorithm. We observe that if node 3 is jammed, whenever a packet from node 1 to node 4 or from node 1 to node 3 arrives at node 2, the node becomes busy since the packet stays in its transmission buffer. The blocked traffic arrival rate at node 2 is $\gamma_{1,3} + \gamma_{1,4}$. We say that node 2 is blocked if its transmission buffer contains at least one blocked packet. If we assume the blocked packet arrival process at node 2 is Bernoulli, the probability that node 2 becomes blocked in a slot is $p = \gamma_{1,3} + \gamma_{1,4}$. Note that if node 2 is blocked at the beginning of a window, then it is blocked throughout the window. If node 2 is not blocked at the beginning of the window, then the probability that it is blocked in the i-th slot of the window is $(1-p)^{i-1}\,p$. Before node 2 is blocked, its busy probability is determined by the equilibrium solution, namely, $P_b(\text{equ})$. After node 2 is blocked, its busy probability is 1

for the remaining time of the window. Therefore, the average busy probability at node 2 can be expressed approximately as:

$$P_b = P_{block} + (1 - P_{block}) \sum_{i=1}^{W} (1 - p)^{i-1} \, p\left(\frac{W - i + 1}{W} + \frac{i - 1}{W} P_b(equ) \right) , \qquad (1)$$

where P_{block} = Prob{node 2 is blocked at the beginning of the observation window}, $P_b(equ)$ is the busy probability due to the modified traffic, and W is the number of slots in an observation window.

Equation (1) is valid for nodes which are the dead-end for some traffic but are not in any routing loop of other traffic; otherwise, the $P_b(equ)$ term must be replaced by $P_b(equ) + (1 - P_b(equ))\, P_b(looping)$. Note that the above derivation is based on the Bernoulli blocked packet arrival process assumption, but the actual process can be complex. The more accurate derivation needs more understanding about the blocked packet arrival process.

Another unique phenomena due to the dead-end node is that when the node is blocked, all traffic flowing through that node is blocked, including the unblocked traffic. Therefore, the equilibrium solution based on the modified traffic model is an upper bound on the packet delay and the busy probability at the good-condition nodes.

V. EFFECT OF LOOPING ON BUSY PROBABILITY

In this section, we examine the effect of looping on the busy probability. The looping-blocked traffic does not stay at any particular node; instead, they move from node to node along the loop.

We first consider the problem of a single routing loop and there is no dead-end node in the loop. The simplest model we can consider is to assume that every blocked packet acts independently and spends equal amount of time in each node in the loop. Thus, for a given blocked packet, the probability that it is at a particular node in the loop in a particular slot is $q = 1/n$, where n is the size of the loop. If there are k blocked packets, the probability that a node contains one or more blocked packet is given by

$$B(k,n) = \sum_{i=1}^{k} (1-q)^{i-1}\, q \quad . \tag{2}$$

Let γ be the rate of the blocked packets entering the loop. then the probability that there are k blocked packets in the loop in an observation window is given by

$$f(N,k) = \binom{N}{k} \gamma^k (1-\gamma)^{N-k} \quad , \tag{3}$$

where N is the total number of slots after the loop was formed and up to the end of the current observation window. Note that the blocked packets entering the loop in the current window affect the busy probability only after their arrival. Thus, the busy probability in the current window depends on the number of blocked packets entering the loop and when these blocked packets arrive. Equation (3) does not take this observation into account. Instead, we assume that all blocked packets entering the loop have the same effect on the busy probability. This assumption simplifies the problem significantly. The busy probability at the node can be approximated by

$$Q(N,n) = \sum_{k=1}^{N} f(N,k)\; B(k,n) \quad . \tag{4}$$

Next, let us consider a node which is in M routing loops, where M > 1. The busy probability due to the blocked packets is given by

$$Q(N,n_1,n_2,\ldots,n_M) = Q(N,n_1) + \sum_{i=2}^{M} \left[\prod_{j=1}^{i-1} (1-Q(N,n_j)) \right] Q(N,n_i) \qquad (5)$$

The above equation is valid because of the assumption that every blocked packet acts independently.

Finally, we have to address the case where there are dead-end nodes in the loop. Note that dead-ends and looping are for different traffic. However, when the dead-end nodes are blocked, the looping-blocked packets are also blocked at the dead-end; thus, the other nodes in the loop do not have the looping-blocked packets any more.

Continuous accumulation of the looping-blocked packets in the nodes along a routing loop may gradually decrease the flow of the unblocked traffic through these ill-conditioned nodes. Therefore, the equilibrium solution based on the modified traffic model is an upper bound on the packet delay and the busy probability at the good-condition nodes.

VI. CONCLUSIONS AND FUTURE RESEARCH

We described and investigated a network analyzer for the PRNETs under nonstatic jamming attack in this report. The analyzer is based on the QNA (Queueing Network Analyzer) algorithm and the modified traffic concept. We illustrated how the blocked packet handling scheme can affect the network operation. We show that the network analyzer can provide a good approximate solution for the Total-Removal scheme. The effects of dead-ends and looping on the busy probability are also investigated. The results presented in this report are based on the assumption of the Bernoulli blocked packet arrival processes.

In the future, we have to assess the accuracy of the proposed network analyzer for various PRNETs under various nonstatic jamming strategies. Other future research topics include improving the accuracy of the network analyzer, incorporating channel monitoring scenario #2 into the network analyzer, and deriving a more accurate model for studying the effects of dead-end and looping.

REFERENCES

[1] U. Cheng, "Static and Dynamic Jamming of Networks," Axiomatix Report No. R8712-6, December 23, 1987.

[2] W. Whit, "The Queueing Network Analyzer," The Bell System Technical Journal, Vol. 62, No. 9, November 1983, pp. 2779 – 2815.

[3] J. A. Silvester and I. Lee, "Throughput/Delay Performance of Multi-Hop Slotted ALOHA Networks," Technical Report CSI-83-09-01, University of Southern California, September 1983.

[4] U. Cheng, "Simulation Study of Periodic Jamming of Adaptive Networks," Axiomatix Report No. R8806-1, June 30, 1988.